ABSTRACT

A cipher communication method by public key cryptosystem, being provably secure and highly efficient, wherein a sender generates ciphertext within a sender device using a receiver's public key and sends the ciphertext over a communication line, and a receiver decrypts the ciphertext using a secret key. For $n=p^dq$ (p and q are prime integers, and pq is k bits), a plaintext space is set to be a subset of an open set $(0,2^{k-2})$ and small residue groups, and an algorithm is formed so that the relationship among solutions of plural second-order equations can be clarified. This has enabled security to be proved by equivalence with the difficulty of the problem of prime factorization, and has achieved faster decryption processing, compared with conventional methods.